



DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5211.6
PERS-00J
14 Apr 08

BUPERS INSTRUCTION 5211.6

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL (BUPERS) COMPLIANCE WITH THE
PRIVACY ACT AND PROTECTION OF PERSONALLY IDENTIFIABLE
INFORMATION (PII)

Ref: (a) 5 U.S.C. 522a
(b) DOD 5400.11-R of 14 May 07
(c) SECNAVINST 5211.5E
(d) Uniform Code of Military Justice (UCMJ)
(e) MILPERSMAN
(f) OPNAVINST 3100.6H
(g) BUPERSNOTE 5239
(h) DON CIO WASHINGTON DC 301540Z Nov 06

Encl: (1) Rules of Conduct Under the Privacy Act

1. Purpose. To implement references (a), (b), and (c) and to ensure that the Bureau of Naval Personnel (BUPERS) and its military, civilian, and contract members are in compliance with the Privacy Act (PA) and protect Personally Identifiable Information (PII). References (d) through (h) provide supporting actions in conjunction with the provisions of this instruction. (Reference (h) is available through the Department of the Navy, Command Information Office (DON CIO) or the BUPERS, Privacy Act/Freedom of Information Act (PA/FOIA) Program Manager.) The Navy must balance its need to maintain information with its obligation to protect individuals against unwarranted invasion of their privacy and the loss or compromise of PII. The Navy must collect, maintain, access, use, transport, disclose, and destroy all personal information and records in a manner consistent with law and regulations. Therefore, BUPERS will employ PA and PII management practices and procedures that evaluate risks and ensure that such material is not lost, stolen, or inappropriately disclosed to the public.

2. Background

a. Reference (a), implemented within the Department of Defense (DOD) and the Department of the Navy (DON) by references (b) and (c), protects the personal privacy of individuals concerning data and other information contained within systems of records maintained by agencies of the Federal Government.

b. The PA's major requirements include, but are not limited to, the following:

(1) All types of records and documents are available to the individual upon request.

(2) Requests for access to one's own record under the PA should be acknowledged within 10 working days of receipt of a written request. (See Requests for Notification and Access to Records in the PA Records System at <http://privacy.navy.mil/privacy/noticenumber/noticeindex.asp>.)

(3) Records requested should be made available to requester within 30 working days of receipt of request. (See paragraph 19.)

(4) Only information that is both necessary and relevant to the business of the agency may be collected and used concerning any individual. It must be maintained in an accurate, relevant, timely, and complete manner.

(5) Individuals have the right to request amendment of their record. Receipt of the amendment request must be acknowledged within 10 working days of receipt.

(6) Generally, disclosure of personal information, other than to the individual and to officials and employees of agencies established as routine users in the Record Systems Notices published in the Federal Register, is not permitted without the written consent of the individual. Detailed disclosure criteria and information are contained in paragraph 19.

(7) An accounting of disclosures to those outside DOD and agencies not covered by an Inter-Agency Support Agreement (IASA) must be maintained. (See paragraph 19.)

c. A command PA team, in addition to individual department efforts, will work to avoid inadvertent releases of PA and PII material.

3. Policy and Scope. DON personnel, including contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, accessing, using, transporting, disclosing, or destroying PA and PII material about an individual. This instruction applies to all military members, civilian employees, and contractors.

4. Rules of Conduct and Criminal Liability of Employees. Enclosure (1) specifies the rules of conduct under the PA that are applicable to all officials and employees in DON. Everyone should be thoroughly familiar with these rules of conduct and the criminal liabilities involved. In particular, the PA provides for criminal sanctions and fines of up to \$5,000 against an official or employee who

a. willfully discloses information protected under the PA to an individual or agency not authorized access to it.

b. willfully maintains a system of records that was not published in the Federal Register.

c. requests, obtains, or receives personal data under false pretenses.

5. Disciplinary and Administrative Actions. In addition to criminal liability, employees who negligently or willfully violate the PA or disregard the provisions outlined in this instruction regarding the handling of PA and PII material may be subject to disciplinary and/or administrative action as follows:

a. Military members. In addition to the criminal penalties of the PA, military members, including reservists on active duty, who violate the provisions of this instruction, may be disciplined per the provisions of references (a) or (d). Additionally, military members may be processed for Administrative Separation per the provisions of reference (e).

b. Civilian Employees. Civilian employees are subject to the criminal provisions of reference (a). Violations of the

provisions of reference (a) or this instruction may result in administrative action.

c. Contractors

(1) When a Navy contract requires the operation of a system of records or a portion of a system of records, or requires the performance of any activities associated with maintaining a system of records, including the collection, use, transport, and dissemination of records, the record system or the portion of the record system affected is considered to be maintained by the Navy. The contractor and its employees are considered employees of the Navy for purposes of the criminal provisions of reference (a) during the performance of the contract.

(2) If the contractor must use, have access to, or disseminate PII subject to references (b) and (c) and this instruction in order to perform any part of a contract, and the information would have been collected, maintained, used, transported, or disseminated by the Navy but for the award of the contract, these contractor activities are subject to references (b) and (c).

6. Terms and Definitions

a. PII Breach. This term is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

b. Lost, Stolen, or Compromised Information. Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will or may be adversely affected. Such incidents are also known as breaches or spillages.

c. Maintain. To collect, maintain, access, use, transport, disclose, or dispose of/destroy PA or PII data or information.

d. Operation of a System of Records. To perform any of the activities associated with maintaining a system of records, including the collection, use, transportation, and dissemination of records.

e. PA Program Manager. Individual appointed by a command to serve as the principal point of contact (POC) on PA matters.

f. Department PA Coordinator. Individual appointed by each department in a command to serve as the principal POC on PA matters and serve as part of the command PA team.

g. Subject Matter Expert (SME). Individual appointed to serve as a specialized consultant on the command PA team.

h. PA Office Administrator. A designated person who has cognizance over any function or program that collects, maintains, or uses PA/PII in a command, department, division, work center, or office.

i. Personally Identifiable Information (PII). Information which can be used to distinguish or trace an individual's identity, e.g. name, social security number, date and place of birth, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, mother's maiden name, other demographics, biometric, personnel, medical, and financial information, etc., including any other personal information which is linked or linkable to a specified individual.

j. Portable Electronic Media. Portable electronic media include, but are not limited to, laptops, flashdrives, thumbdrives, CD/DVD, diskettes, and Blackberries.

k. Privacy Act Statement (PAS). A statement which outlines the individual's rights required to be posted whenever an individual is requested to furnish personal information for inclusion in a system of records regardless of the medium used to collect the information (paper or electronic forms, personal interviews, telephonic interviews or other methods). The statement enables the individual to make an informed decision whether to provide the information requested. A PAS shall include all of the elements found in reference (b), section C2.1.4.2.

l. Privacy Impact Assessment (PIA). An assessment to evaluate adequate practices to balance the privacy concerns of the individual against the security needs of the organization. The process is designed to guide owners and developers of information systems in assessing risks to personal privacy during the early stages of development. The process consists of privacy training, gathering data from a project or privacy issues, identifying and resolving the privacy risks, and approval by the command Information Assurance Manager (IAM).

m. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DON activity including, but not limited to, the individual's personnel, medical, financial, or criminal history, etc., and that contains the individual's name or other identifying particulars assigned to the individual, such as a social security number, date of birth, finger or voice print, or a photograph.

n. System of Records Manager. An official who has overall responsibility for a system of records. They may serve at any level in DON. System of records managers are annotated in the published record systems notices. If more than one official is indicated as a system of records manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records, at the local activity).

o. System of Records. A group of records under the control of a DON activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all PA systems of records must be published in the Federal Register and are also available for viewing or downloading from the Navy's Privacy Act Online Web site <http://privacy.navy.mil>.

7. Action. The following functions will be performed as described below:

a. Privacy Act Coordination Office. Each command will have a centralized office and POC to provide guidance and assistance, where applicable, in administering the Privacy Act of 1974. Overall responsibilities of this office are as follows:

(1) Develop overall command policy relative to the PA.

(2) Broadly monitor command compliance with DOD and DON PA instructions.

b. Command Privacy Act Program Managers

(1) Develop materials such as forms, reporting formats, and directives for implementation of the PA. Consolidate data and make required reports, including denials of PA requests. Ensure training programs required by the PA are accomplished. Process requests and maintain processing logs for notification, access, and amendment under the PA. Coordinate with responsible department PA coordinators or directly with other employees as required, and obtain assistance, when necessary.

(2) Provide a brief overview of the PA and provide a copy of the current PA training module to new command personnel during check-in. Provide PA refresher training material to department PA coordinators for their use in additional department-level training as applicable.

(3) Head the command privacy team. Communicate on a regular basis with department PA coordinators to ensure compliance with the Navy's PA Program.

(4) Process formal PA complaints.

(5) Serve as a designated command official in reporting and providing necessary additional actions regarding PA and PII breach incidents.

(6) Annually require that department heads review their applicable system of records notices to ensure that such notices are necessary, accurate, and complete.

c. Departments Heads. Each department head will ensure that the following specific duties are carried out in their department:

(1) Ensure the commanding officer, executive officer or deputy, and the command designated representative for PII breaches are notified immediately once they become aware of a reportable incident.

(2) Respond promptly to requests from the command PA program manager or the applicable department PA coordinator for access, copies of records, or amendment action concerning records within the department.

(3) Bi-annually review and revise, as appropriate, all command articles, instructions, notices, manuals, and business processes under the department's responsibility to meet the requirements of the PA.

(4) Monitor the relevance, accuracy, timeliness, and completeness of records and data elements for which the department is responsible.

(5) Ensure records containing PA and PII material within the department are stored and disposed of as specified in paragraph 14.

(6) Ensure that requests for personnel record data are released under current procedures. If uncertain as to whether or not disclosure of data is authorized under the PA, contact the command PA program manager for assistance.

(7) Ensure that an accounting of disclosures made to agencies outside DOD and with whom IASAs do not exist, is recorded on OPNAV 5211/9, Disclosure Accounting Form, and filed in the applicable record. Additional guidance is contained in paragraph 19.

(8) Draft PA statements for those forms under the department's cognizance that require such statements. Chop through the command records manager/forms manager as appropriate and the command PA program manager prior to submitting for printing.

(9) Provide PA program guidance to department personnel who solicit and award or administer government contracts; and inform prospective contractors of their responsibilities regarding the DON PA Program. This activity should be coordinated with the command contract specialist SME.

(10) Establish contract surveillance programs for the department to ensure contractors comply with the procedures established by Defense Acquisition Regulatory (DAR) Council.

This activity should be coordinated with the command contract specialist SME.

(11) Review annually or more frequently the necessity of the use of laptops and portable electronic media (e.g., flashdrives, thumbdrives, CD/DVD, diskettes, and blackberries) by department personnel.

(12) Work closely with the public affairs officer and/or Web master to ensure that PA and PII material is not placed on public Web sites or in public folders.

d. Department Privacy Act Coordinators. Each department head will designate, in writing, a department PA coordinator who will function as the department's POC on PA and PII matters noted below and will be a member of the command privacy team. Department PA coordinators will be the rank of O4 or above or a civilian equivalent grade, if possible. This assignment is a significant collateral duty, and an important component of a department's compliance with the PA. For the purpose of the PA, department PA coordinators report directly to the PA program manager. Specific duties of department PA coordinators are as follows:

(1) Provide PA refresher training as necessary to department personnel utilizing PA training material provided by the BUPERS/Navy Personnel Command (NAVPERSCOM) PA Program Manager. Provide the command PA program manager with an accounting of department personnel who complete refresher training. The department PA coordinator will ensure that all department personnel complete PA refresher training as necessary.

(2) Communicate on a regular basis with the command PA program manager to discuss department PA issues, provide suggested solutions to PA problems, and provide updates to ongoing PA initiatives.

(3) Conduct monthly visits to applicable department office spaces to ensure that personnel are safely disposing of PA and PII material and following other recommended best practices as outlined in the training material published by Director, Navy Staff (DNS-36). NAVPERS 5211/15, Bureau of Naval Personnel Privacy Act Coordinator Checklist, should be utilized

during such visits, and maintained for a period of 2 years. The command PA program manager should be provided a copy of completed forms for inspection upon request.

e. Subject Matter Experts (SMEs). In addition to department PA coordinators, SMEs will also be appointed as part of the command privacy team. At a minimum, the command privacy team will include a designated records management official, a contract specialist, and an information technology specialist.

f. Public Affairs Office (PAO)

(1) The command PAO will take all necessary steps to prevent the posting of PA and PII material to their command publicly-accessible Web sites.

(2) Command PAOs will prepare responses to query (RTQ) for PA and PII breach incidents originating from their commands.

g. Command Information Officer (CIO)/IAM

(1) Provide guidance for the effective assessment and utilization of privacy-related technologies.

(2) Provide guidance on the conduct of PIAs and oversee command PIA policy and procedures to ensure PIAs are conducted commensurate with the information system being assessed, the sensitivity of PII in that system, and the risk of harm for unauthorized release of that information. DON CIO reserves the right to request that a PIA be completed on any system that may have privacy risks.

(3) Review all command PIAs prior to approval by the DON CIO.

(4) Develop and coordinate privacy policy, procedures, education, training and awareness practices with the PA program manager regarding command information systems.

14. Safeguarding Personal Information

a. The Privacy Act of 1974 requires that certain safeguards be taken to ensure the security and confidentiality of personal

information contained in various records systems maintained by commands.

b. If the inadvertent or unauthorized disclosure of personal information or records will result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such records must be given proper protection against hazards to their security or integrity.

c. Generally, limited access to buildings after working hours will suffice relative to the storage of personnel records, etc. Records containing PA and PII material must be stored so that they cannot be openly viewed, with the exception of material in the selection board area that has other security precautions in effect.

d. Per reference (c), records containing PA and PII material must be disposed of by rendering the material unrecognizable or beyond reconstruction (e.g., burning, chemical decomposition, shredding, or mutilation). Each command may have more specific established protocols to ensure that PA and PII material is properly destroyed.

15. Management of Privacy Act (PA) and Personally Identifiable Information (PII)

a. Access/Disclosure. Access to and disclosure of PA and PII material must be strictly limited to individuals with an official need to know. It is inappropriate to use PA/PII in group/bulk orders. Appropriate actions must be taken to protect PA and PII material from being widely disseminated. In particular, PA and PII material shall not be posted on electronic bulletin boards because the PA strictly limits PA and PII access to those offices and employees of the agency with an official need to know.

b. Transmittal. In those instances where transmittal of PA and PII material is necessary, the originator must take every step to properly mark the correspondence so that the receiver of the information is apprised of the need to properly protect the information. For example, when transmitting PA and PII material in a paper document, fax, or e-mail, it is required to mark it "FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal

penalties." When sending a message that contains PA and PII material, it should be marked FOUO. It is also advisable to inform the recipient that the message should not be posted on a bulletin board. Per paragraph 15a, PA/PII shall not be posted on electronic bulletin boards.

c. Portable Electronic Media. Reference (g) provides current guidance regarding the management of all unclassified Data at Rest (DAR) and data in transmission that has not been approved for public release and is stored on mobile computing devices. Reference (g) will continually update applicable BUPERS Component policy. Echelon III Information Assurance Managers (IAM) are responsible for and will provide training on the proper encryption process within their commands. NAVPERS 5211/14 will be completed when obtaining approval for the removal of portable electronic media from a DOD owned, leased, or occupied workplace. Additionally, a proper inventory of PII contained on the portable electronic media must be captured prior to removal from a DOD owned, leased, or occupied workplace so that negatively impacted individuals may be identified and contacted if a breach of the PII material occurs.

d. Portable electronic media must be protected at all times. Individuals using and/or traveling with laptops and portable electronic media will maintain positive control of the laptop and media at all times. Laptops and portable electronic media will not be placed in checked luggage or left in unoccupied vehicles at any time. Laptops and portable electronic media will be secured inside a locked room and if available stored in a locked container when utilizing government, commercial or private lodging.

e. Do not maintain/store/process PA and PII material on personal or non-government owned/provided/authorized computers (including hotel, internet café, library, or other non-government computers), network systems, or portable electronic media (i.e., laptops, flashdrives, thumbdrives, CD/DVD, diskettes, blackberries), or other portable electronic devices.

f. Collection/Maintenance. The collection and maintenance of information retrieved by an individual's name and/or personal identifier should be performed in compliance with the appropriate PA systems of record notice (<http://www.privacy.navy.mil>). If required to collect and maintain information retrieved by an

individual's name and/or personal identifier, there must be an approved PA systems notice to cover that collection. If unsure as to whether a systems notice exists or not, contact the command PA program manager for assistance.

g. Unauthorized Disclosure. In the event of an actual or potential loss, theft, or compromise of PA and PII material, including breaches and spillages, departments shall take immediate action, per reference (h), to prohibit further damage/disclosure and will immediately report the breach to their commander, deputy commander, and the designated breach reporting official, typically the command PA program manager. The designated command official will immediately file a Breach Notification e-mail as follows based on input from the command department in which the breach occurred:

(1) Within 1 Hour. Notify, by a single e-mail, per reference (b), section C10.6: the United States Computer Emergency Readiness Team (US-CERT), e-mail: soc@us-cert.gov, copy to DON CIO, e-mail: don.privacy.fct@navy.mil, the Defense Privacy Office, e-mail: dod.privacy@osd.mil and pia@osd.mil, and the Chief of Information (CHINFO), e-mail: chinfo.dutyoffic.fct@navy.mil. If appropriate, issue OPREP-3 per reference (f). E-mail shall contain the information requested in reference (b), section C10.6: component/organization involved; date of incident; number of individuals impacted and if government civilian, military and/or private citizens (including percentage of each category); brief description of incident including circumstances, information lost or compromised, and if PA and PII material was encrypted and/or password protected.

(2) If criminal intent is suspected, notify the local Naval Criminal Investigative Service (NAVCRIMINSERV) office. Contact the local Staff Judge Advocate (SJA) or Office of General Counsel (OGC) if their office is not submitting the breach report.

(3) Within 10 Days. The DON CIO Privacy Office will review the initial breach report and determine, using DOD's risk analysis methodology, the potential risk of harm to impacted personnel. The DON CIO Privacy Office will apprise the organization's designated breach official as to what notifications, if any, are required. If notifications are required, they must be made within 10 days of the discovery of

loss or suspected loss of PII. Notification must be made by the designated breach official by written letter or digitally signed e-mail to all impacted individuals with full administrative support by the department in which the breach occurred. If unable to notify individuals within 10 days, report to DON CIO Privacy Office the reasons why notification was not made and actions being taken to complete notification process. When impacted personnel cannot be located or directly contacted, the command/activity should use any means that will likely succeed in reaching the impacted individuals, such as establishing a toll-free number (i.e., call center) per guidance provided at <http://privacy.navy.mil>. For all incidents that require notification, the command/activity is directed to investigate whether DON policy was followed. In cases where policy was not followed, disciplinary action should be considered, weighing mitigating circumstances, severity of the PII loss or compromise, and other extenuating factors.

(4) Intermediate Reporting. As soon as additional breach information becomes available, the designated breach official will submit this information to the DON CIO Privacy Office via e-mail.

(5) Within 30 days. The designated breach official will send lessons learned, remedial action taken to prevent reoccurrence, and disciplinary action taken, where appropriate, via e-mail to the DON CIO Privacy Office.

16. Requests for Notification and Access to Records in the PA Records System

a. Any request for notification, access, or copies of records or documents that cite the PA must be hand-carried, mailed, or e-mailed for expeditious processing to the command PA program manager due to time constraints imposed by the Act.

b. Routine requests for copies of records not citing the PA should continue to be handled per other current instructions.

c. Any requests for access or copies of any documents or records from the individual (not third party requests) and citing the Freedom of Information Act (FOIA) must also be hand-carried, mailed, or e-mailed to the command PA program manager for expeditious handling due to time constraints. FOIA requests

from individuals asking for their own records will be treated as PA requests.

d. The command PA program manager will accomplish processing of correspondence submitted under the PA. This includes sending acknowledgment to the requester, tracking requests, collecting requested information from responsible organizations, and responding to the requester.

e. In collecting the information requested by the individual, the command PA program manager will send a copy of the request to the responsible office POC, who will then search and forward the material requested.

(1) If access has been requested, arrangements will be made to make material available at a specified time.

(2) If copies have been requested, the responsible office will make the copies and send them to the command PA program manager. The material must be screened to ensure that the privacy of other individuals is maintained. For example, a message filed in the individual's record that contains data concerning several individuals must be photocopied so the names of all individuals except the subject of the record are blocked out. Office POCs are strongly encouraged to bring any records to the command PA program manager where there is a question of what should or should not be copied. Office contacts are reminded that there are few exemptions for withholding any PA record information from the requesting individual.

(3) If any material appears to be covered by an exemption, the command PA program manager will review the material in question for a final determination.

17. Requests for Amendment

a. Routine requests for error correction and changes to records not involving the PA should be processed per other current procedures. The command PA program manager should not become involved in the normal, day-to-day routine operations of the organization.

b. If any department receives a request to change, amend, or delete any record, document, or data element, and the PA is

invoked, the request must be hand-carried, mailed, or e-mailed to the command PA program manager immediately. (Time constraints on processing amendment requests are extremely critical.)

c. The command PA program manager will process amendment requests. When a request for amendment has been received the request will be sent to the command action office for the initial recommendation as to whether or not the amendment request should be granted.

(1) If additional documentation is not required and the decision is to grant the amendment, the amendment will be made. The applicable action office will ensure that the amendment is made. When the amendment has been made, a copy of the completed action will be provided to the command PA program manager by the due date specified. Extensions cannot be granted except in extreme circumstances due to the critical time constraints imposed by the Act.

(2) If additional documentation or clarification is required to process the request or amendment, provide a statement requesting same in finished format, along with the request to the command PA program manager for inclusion with response to the requester.

(3) If the responsible office believes that the amendment requested should not be granted, this should be conveyed back to the command PA program manager in writing (with the reasons and citations of existing instructions supporting the determination not to amend). The command PA program manager will make a final decision on amendment in these cases.

18. Statement of Dispute

a. If denial of a request for amendment is upheld through the review process, the individual is entitled to file a statement of dispute with the PA system manager setting forth the reasons for the individual's disagreement with the refusal of the agency to amend the record.

b. The record (including computer data elements) must be clearly annotated so the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose

it. The notation itself should be integral to the record and specific to the portion in dispute. Computer files may be cross-referenced to a paper statement of dispute on file.

c. When the record or portion of the record to be disclosed is the subject of a statement of dispute, a copy of the individual's statement must be provided to the user. Also, to the extent an accounting of disclosures was maintained, a copy of the statement dispute must be sent to prior recipients of the record or portion of the record involved.

19. Release of Information and Accounting of Disclosures

a. Previous regulations concerning the release of information from the personnel records of members and former members of the naval service permitted disclosure of certain personal information when a specific purpose under those regulations was stated. In many instances, these disclosures are no longer permitted by the Privacy Act of 1974 without the written consent of the individual. Any department receiving such an inquiry should consult their command PA program manager.

b. Generally, information can be released on a need-to-know basis to other organizations within DOD.

c. Duty officers generally should not divulge information from personnel records. Few requests for such information are so urgent that they cannot be held for processing through established channels during the next working day. In any event, FOIA-type personnel records information only will be released. Front office personnel to include the commanding officer, executive officer, commander, deputy commander, executive assistant, deputy executive assistant, flag secretary, and command master chief will immediately be provided with requested phone recall information (work, home, and cell phone numbers). Other requested information such as home address and social security numbers will be promptly provided via the appropriate Navy e-mail account. All duty watch personnel will be familiar with the front office personnel in their chain of command.

d. An accounting of each disclosure of information from an individual's record must be recorded and maintained unless either of the following conditions applies:

(1) The information is released to officials and employees of DOD (if the need-to-know is established).

(2) The information is requested and releasable under the FOIA (e.g., for information normally releasable to the public).

e. Generally, an accounting of disclosures of personnel record information outside DON or DOD, even to a routine user as published in Record Systems Notices, requires an accounting of the disclosure. OPNAV 5211/9 is to be used for manually maintained records.

f. If, however, there is an IASA between organizations and another agency (e.g., Department of Veterans' Affairs), then the exchange of personal information (e.g., verification of service for veterans' benefits) is considered to be an intra-agency disclosure.

20. Forms

a. OPNAV 5211/9 (03-92), Disclosure Accounting Form is available at <https://navalforms.daps.dla.mil/web/public/home>.

b. NAVPERS 5211/14 (08-07), Bureau of Naval Personnel Sign Out/Sign in Form for Portable Devices Containing Privacy Act/Personally Identifiable Information, and NAVPERS 5211/15 (08-07), Bureau of Naval Personnel Privacy Act Coordinator Checklist are available at <http://www.npc.navy.mil/ReferenceLibrary/Forms/NAVPERS/>.

E. MASSO
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
Electronic only, via BUPERS Web site
<http://buperscd.technology.navy.mil/>

RULES OF CONDUCT UNDER THE PRIVACY ACT

1. Maintaining Personnel Records. It is unlawful to maintain systems of records about individuals without prior announcement in the Federal Register. Anyone maintaining these records is subject to criminal penalties up to \$5,000. Even with such notice, care will be taken to keep only the personal information necessary to do what the law and the President, by executive order, require. The information is to be used only for the purposes described in the Federal Register.

2. Disclosure. Information about an individual will not be disclosed to any unauthorized individuals. Anyone who makes an unauthorized disclosure on purpose may be fined up to \$5,000. Every member or employee of the Department of the Navy (DON) who maintains records about individuals has an obligation to do their part in protecting personal information from unauthorized disclosure. SECNAVINST 5211.5E describes when disclosures are authorized.

3. Individual Access. Every individual, with certain exceptions, has the right to look at any PA record the DON keeps on them, to copy it, and to request to have it corrected if they consider it wrong. The individual attempting to exercise these rights will be given courteous and considerate assistance.

4. Ensuring Accuracy. The DON has an obligation to use only accurate, timely, relevant, and complete information when making decisions about individuals. Every member, official, and employee involved in keeping records on individuals will assist in the discharge of this obligation.